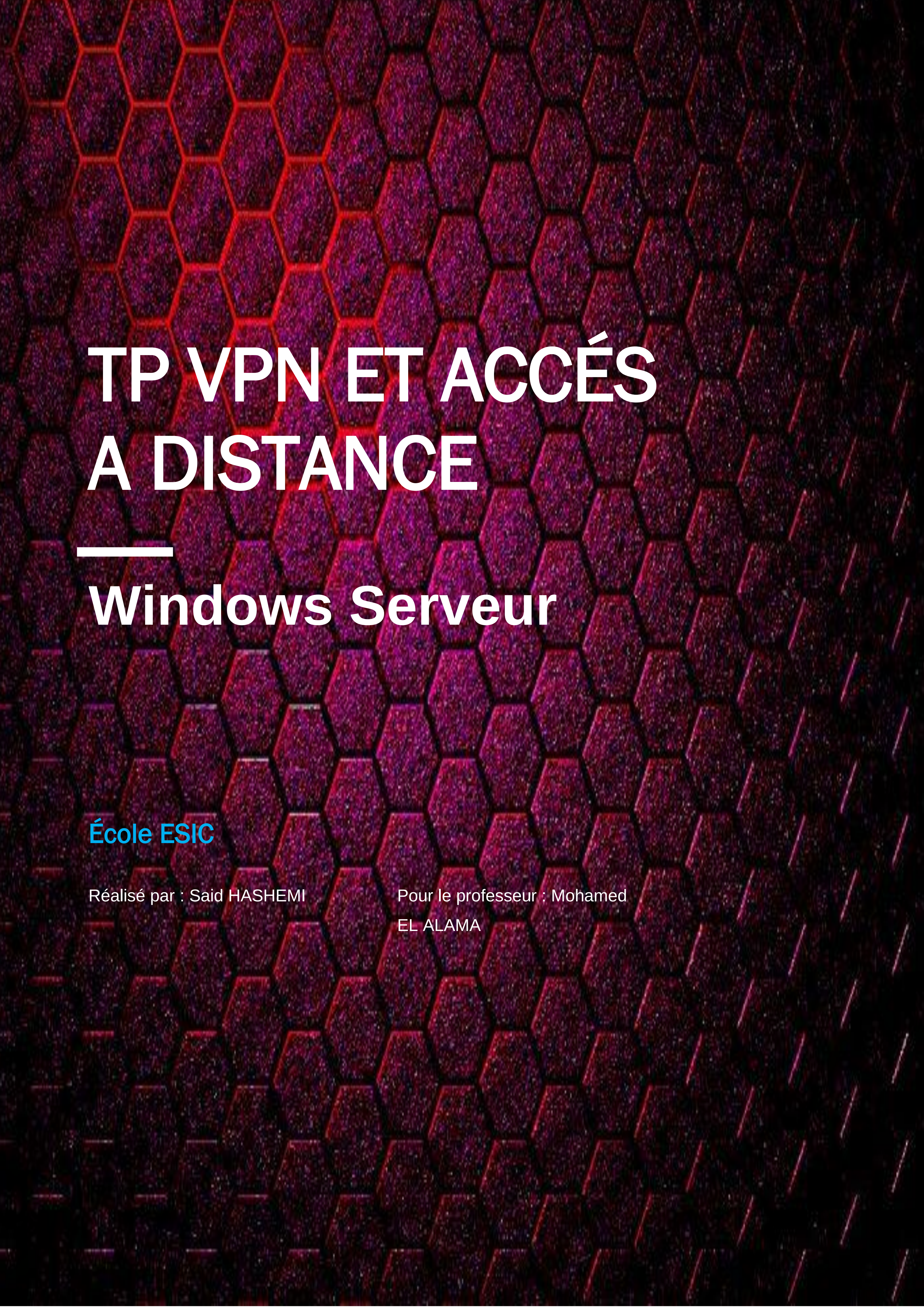


TP VPN ET ACCÉS A DISTANCE

Windows Serveur

École ESIC

Réalisé par : Said HASHEMI

Pour le professeur : Mohamed EL ALAMA

Objectif

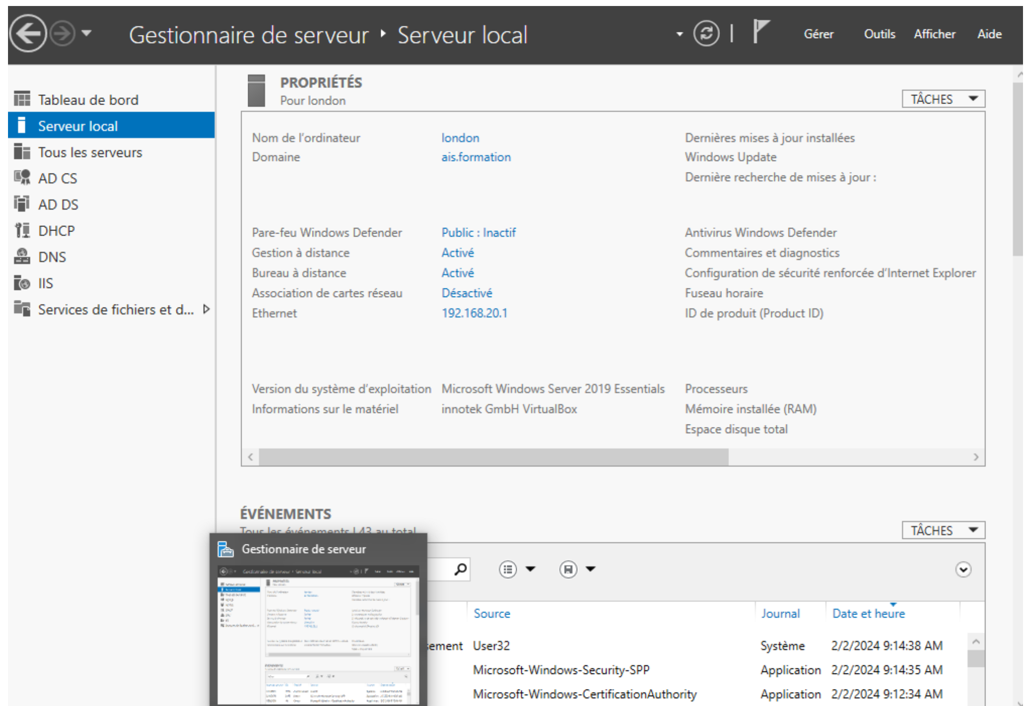
L'objectif de TP VPN et accès à distance sur Windows Server 2019 pour l'école ESIC est de créer une infrastructure sécurisée permettant aux utilisateurs distants d'accéder de manière fiable et sécurisée aux ressources du réseau. Tout d'abord, on devra analyser en détail les besoins spécifiques pour mettre en place le service d'accès distant, en identifiant les services essentiels à rendre accessibles. Ensuite, en suivant une approche méthodique, ils devront concevoir et configurer le serveur VPN, en choisissant les protocoles appropriés et en mettant en place des politiques de sécurité robustes. La gestion des utilisateurs, les tests approfondis de connectivité, et la documentation complète seront des composants essentiels de ce projet. Une fois achevé, le système devrait non seulement permettre un accès distant sécurisé, mais également être maintenable et évolutif pour répondre aux futurs besoins.

Table de matières

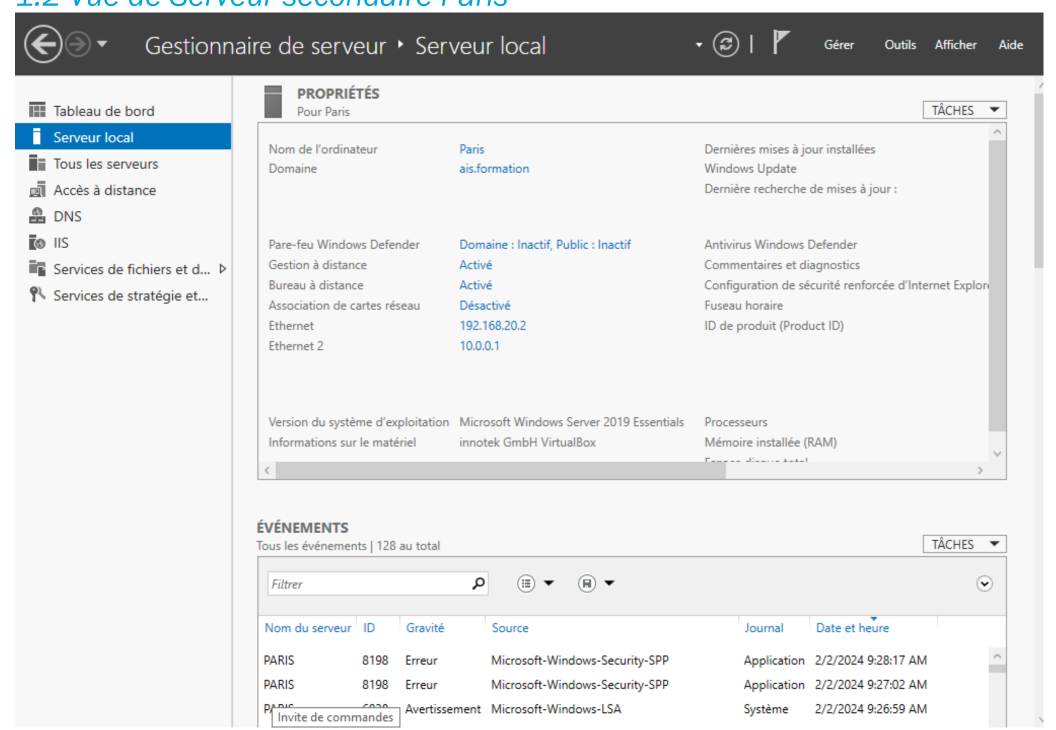
1. Introduction

Nous disposons de deux serveurs, le serveur principal baptisé London et le serveur secondaire nommé Paris. Le serveur principal a été configuré avec toutes les fonctionnalités nécessaires telles qu'AD DS, DNS, DHCP, etc. Quant au Serveur Secondaire, il a été mis en place en tant que DNS secondaire, et on va installer les fonctionnalités d'accès à distance et NPS sur ce serveur.

1.1 Vue de serveur London



1.2 Vue de Serveur secondaire Paris



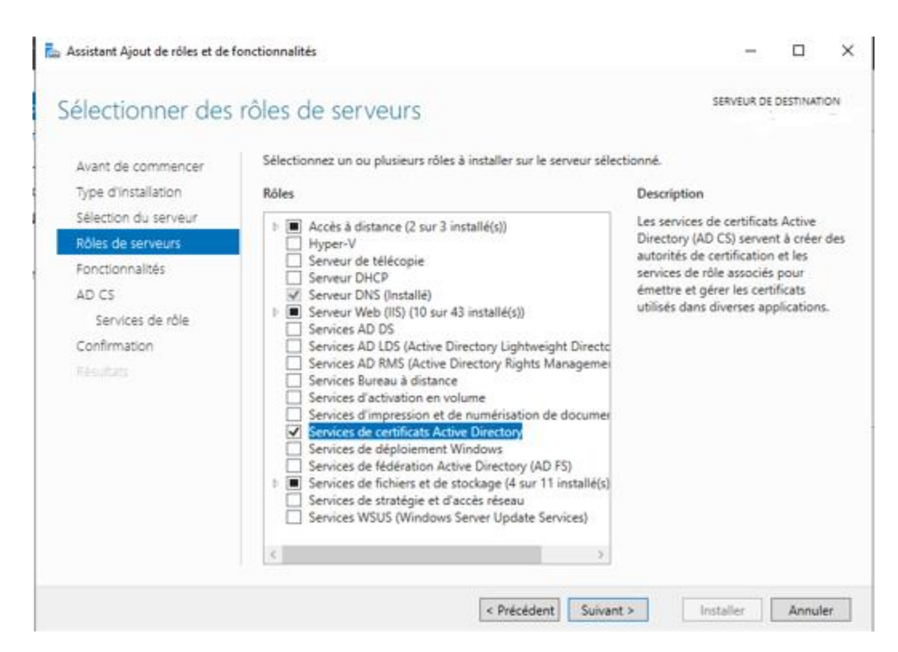
On va configurer une VM au nom de « Client », avec l'adresse IP 10.0.0.2 pour ce TP.

2. Installation de la fonctionnalité AD CS

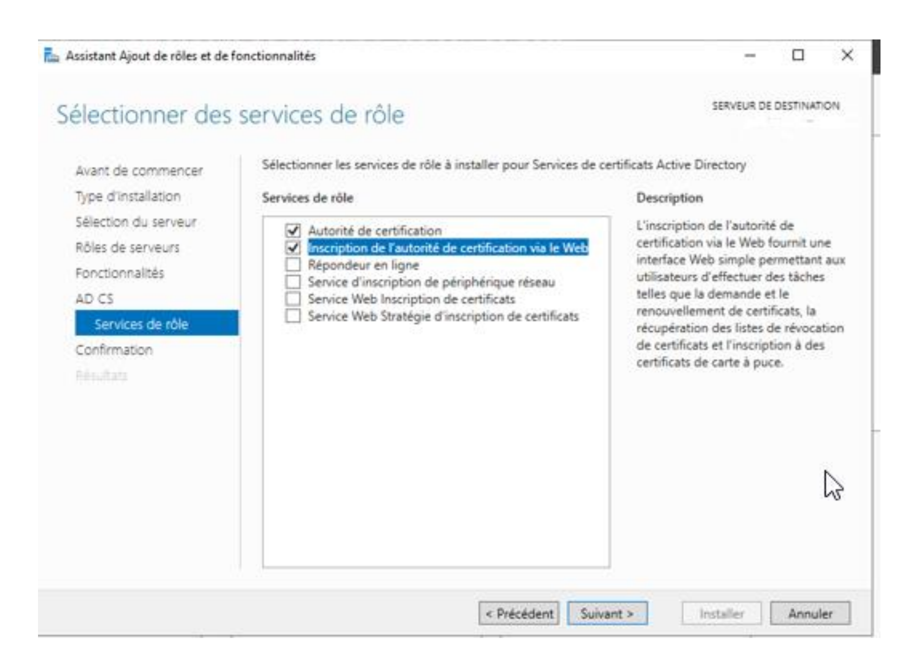
AD CS (Active Directory Certificate Services) est une fonctionnalité de Windows Server qui permet de créer, distribuer et gérer des certificats de sécurité dans un environnement Active Directory. Les certificats sont utilisés pour sécuriser les communications, notamment dans les services tels que SSL/TLS. On va installer cette fonctionnalité sur le serveur London.

2.1 Étapes d'installation

Depuis le menu "Gestionnaire de serveur", ajoutons le rôle "Services de certificats Active Directory".

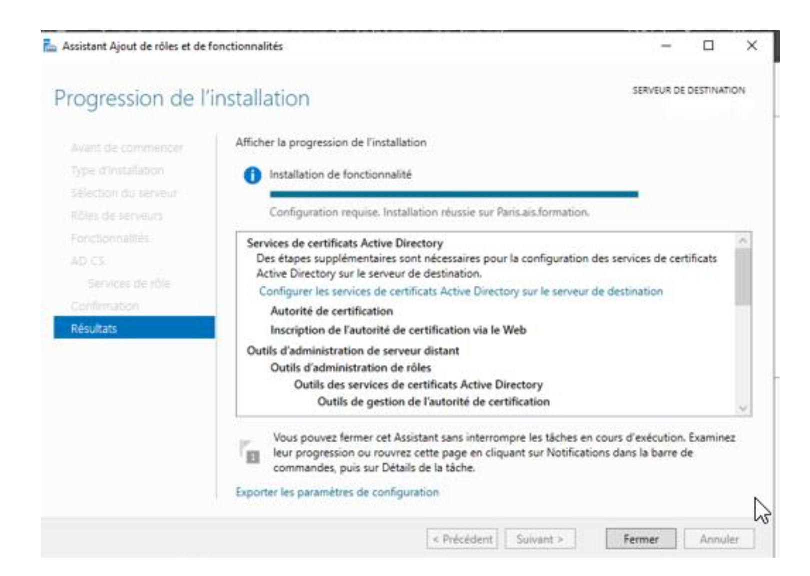


Choisissons maintenant Autorité de certification (CA) et Autorité de certification en ligne (CA Web). La première émet des certificats, la seconde offre un portail web pour les demandes de certificats.



Choisissons où stocker les clés privées des certificats. Une option importante pour la sécurité.

On va Laisser l'assistant installer les services nécessaires. Cela inclut le service de certificat et éventuellement le service web si vous optez pour une CA Web.



2.1.1 Configuration finale

Finalisons la configuration en fonction des spécifications de notre environnement, telles que les options de chiffrement, les durées de validité des certificats, etc.

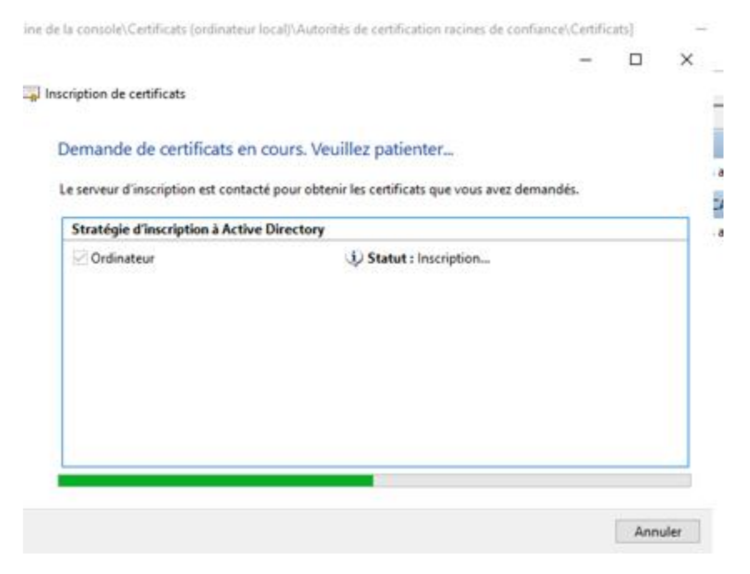
On doit définir les autorisations pour les administrateurs et les utilisateurs finaux en fonction des tâches qu'ils doivent accomplir.

2.2 Demander un certificat pour le Serveur secondaire Paris

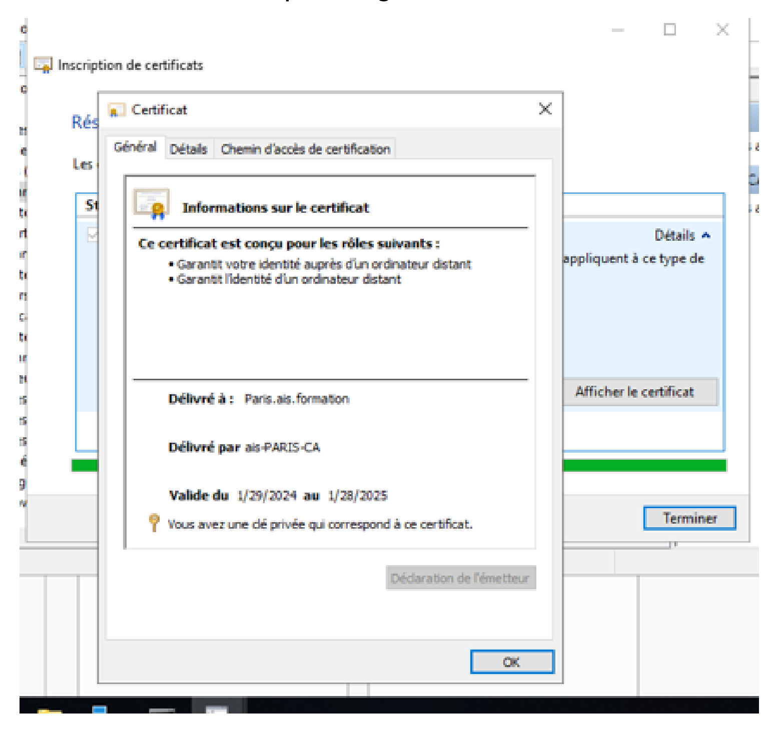
Tout d'abord Il faut vérifier d'avoir les droits nécessaires pour demander un certificat.

Sur le serveur secondaire, on va ouvrir la console de gestion AD CS ou dans l'invite des commandes on tape mmc ensuite on ajoute la fonctionnalité « autorité des certificats » sur mmc.

On développe l'option « certificat » et on clique sur « personnel » et ensuite sur « nouveau » pour demander un certificat.

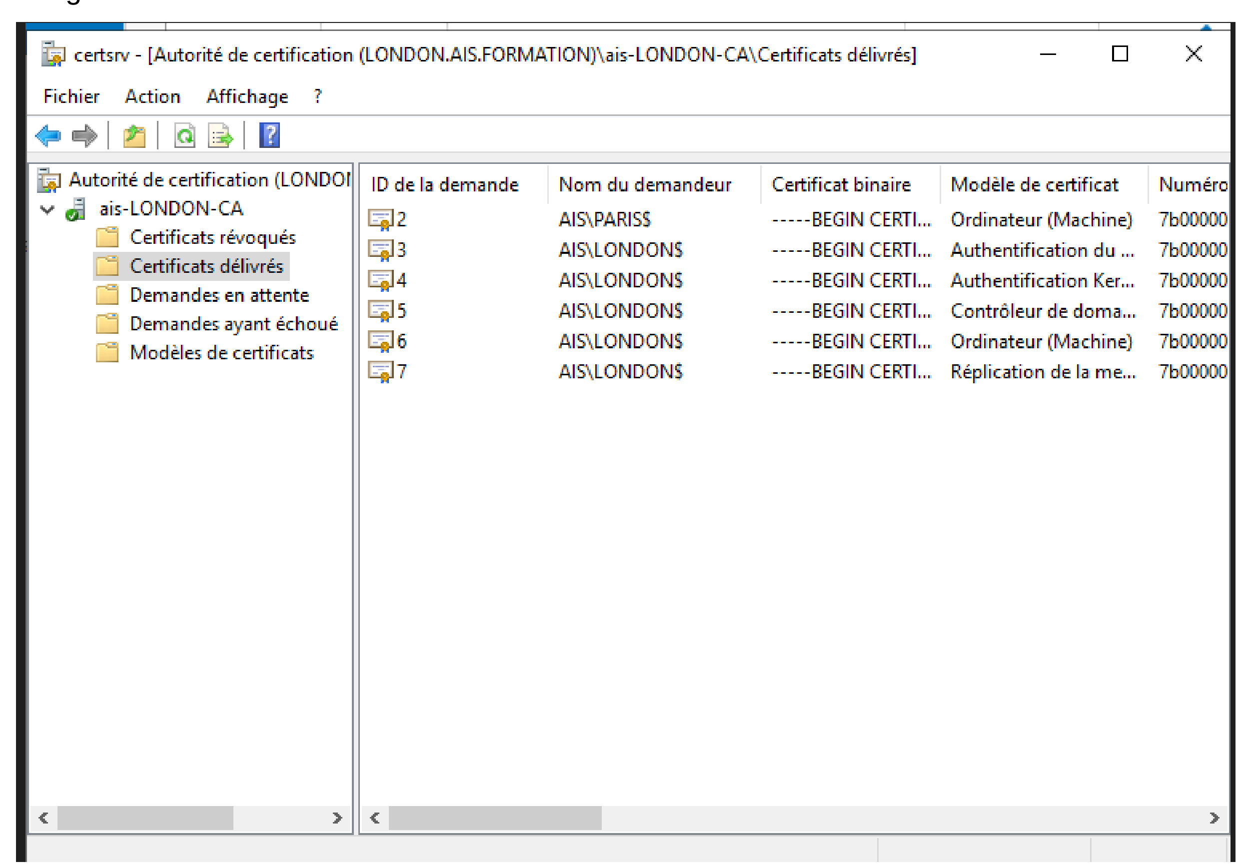


Une fois installé, on peut regarder le certificat délivré :



On a bien enregistré le certificat, maintenant il faut qu'on installe le NPS et le Service d'accès à distance un par un sur le serveur Paris.

Image de certificat délivré :

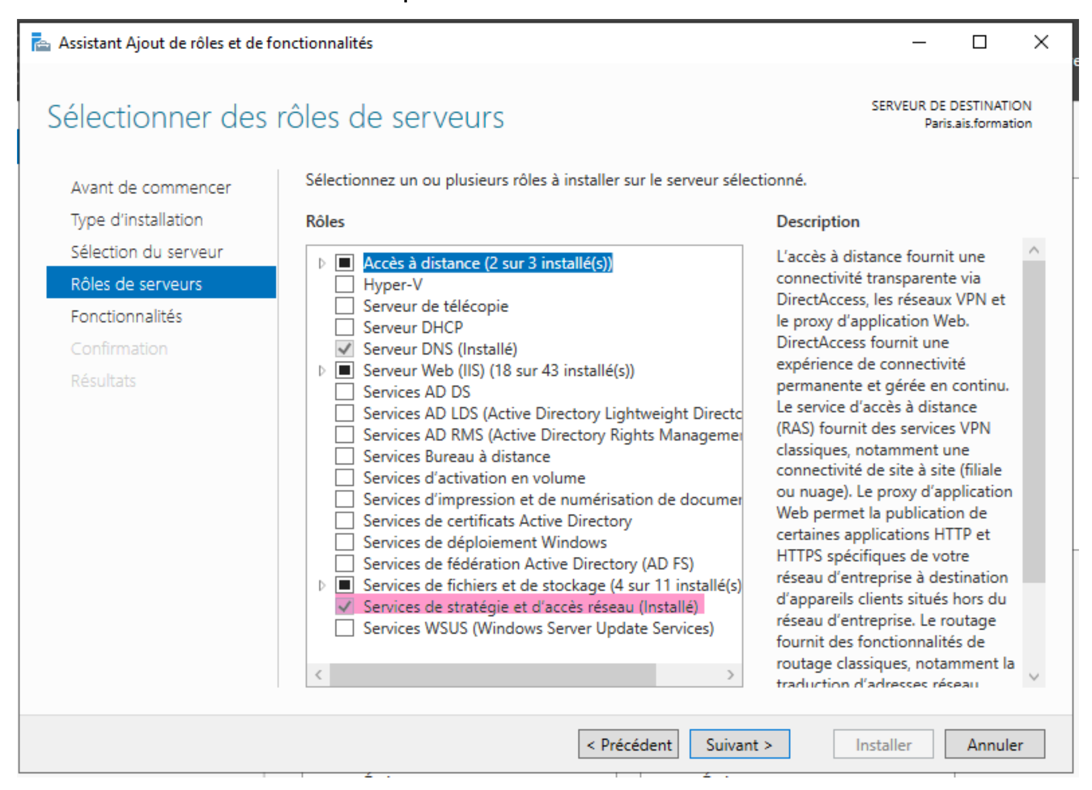


3. Installation de la rôle NPS

Network Policy Server est un service essentiel dans Windows Server qui gère l'authentification, l'autorisation et la comptabilité pour les connexions réseau, contribuant ainsi à sécuriser et gérer efficacement l'infrastructure réseau.

Pour installer la rôle NPS, on va suivre ces étapes :

- Accéder au Gestionnaire de serveur sur votre serveur Windows.
- Sélectionner "Ajouter des rôles et fonctionnalités".
- Choisir "Services de stratégie d'accès réseau" (Network Policy and Access Services) et suivre les instructions pour installer le service NPS.

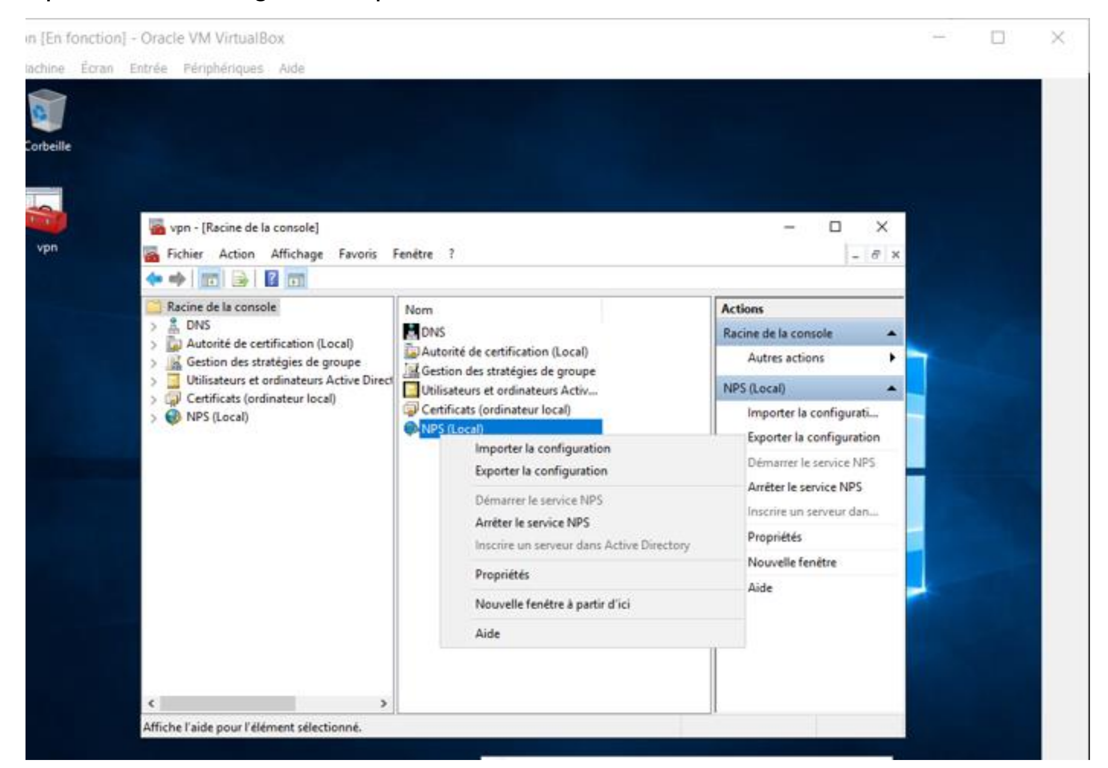


3.1 Configuration de NPS

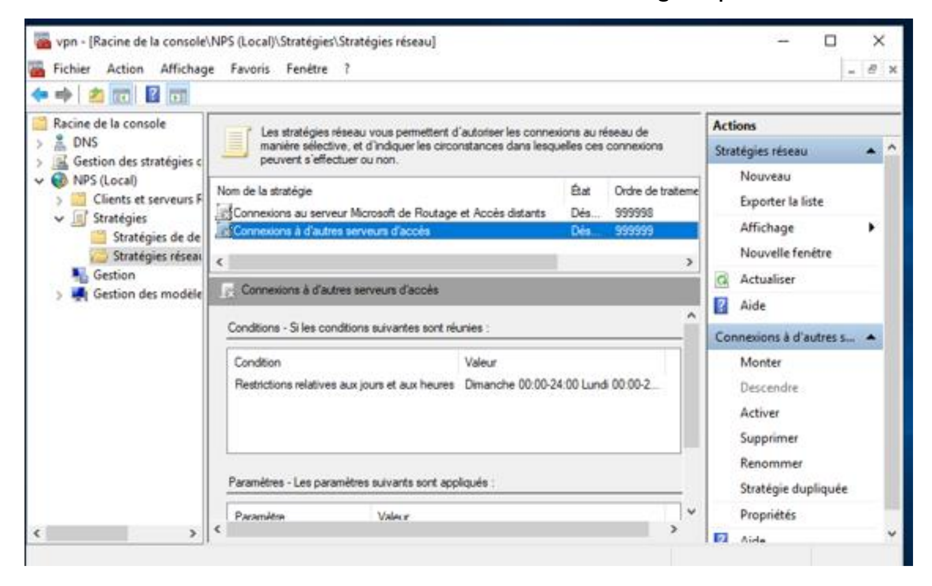
Après l'installation, on va ouvrir le Gestionnaire NPS depuis l'outil d'administration.

Dans le volet gauche, il faut sélectionner "Serveurs NPS" et cliquer avec le bouton droit pour ajouter le serveur sur l'AD.

Après on va configurer les paramètres de base. On démarre le NPS :

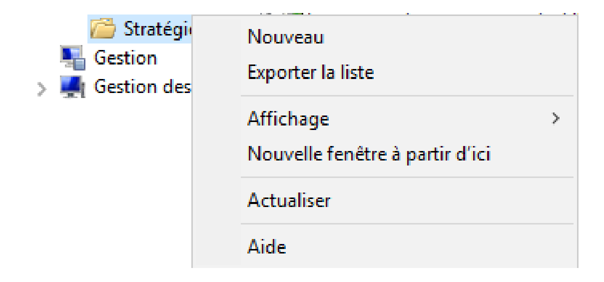


Maintenant on doit définir des stratégies réseau pour spécifier comment le NPS doit traiter les connexions. Pour ce faire on désactive les stratégies par défaut.

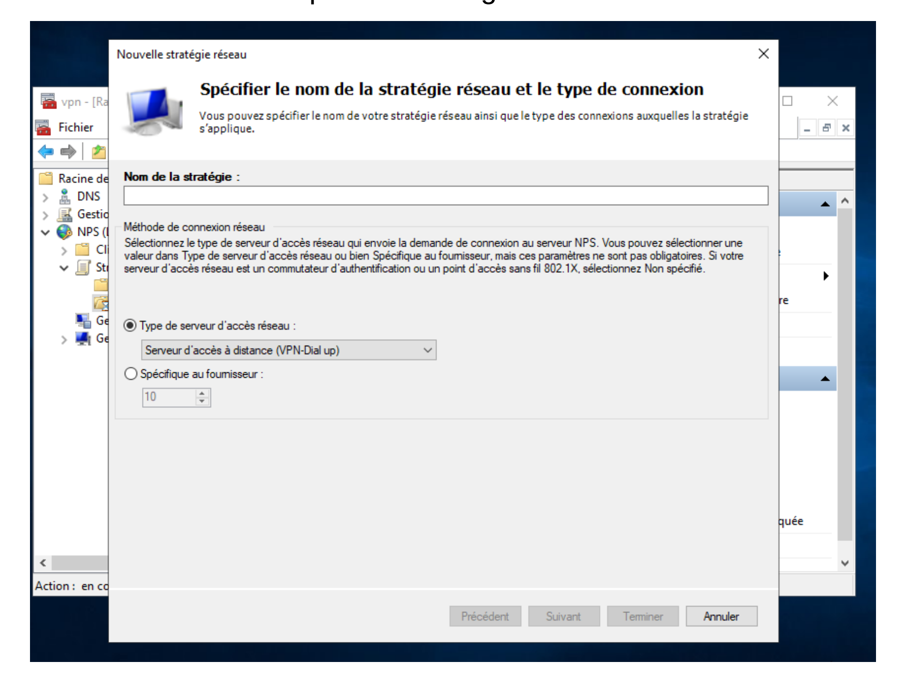


Et ensuite il faut créer des règles d'accès, des conditions et des profils d'authentification pour déterminer l'autorisation des utilisateurs et des dispositifs.

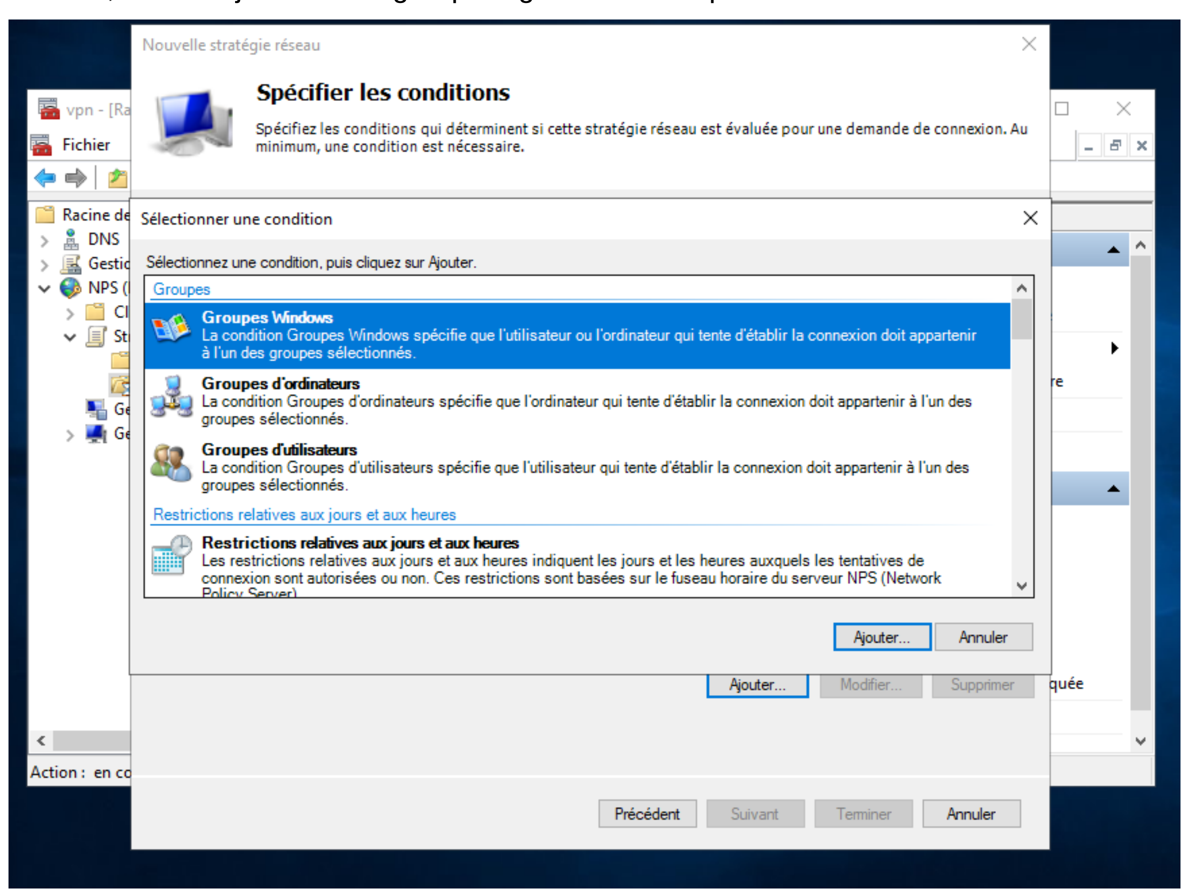
Pour créer une nouvelle stratégie, on clique sur « nouveau » :



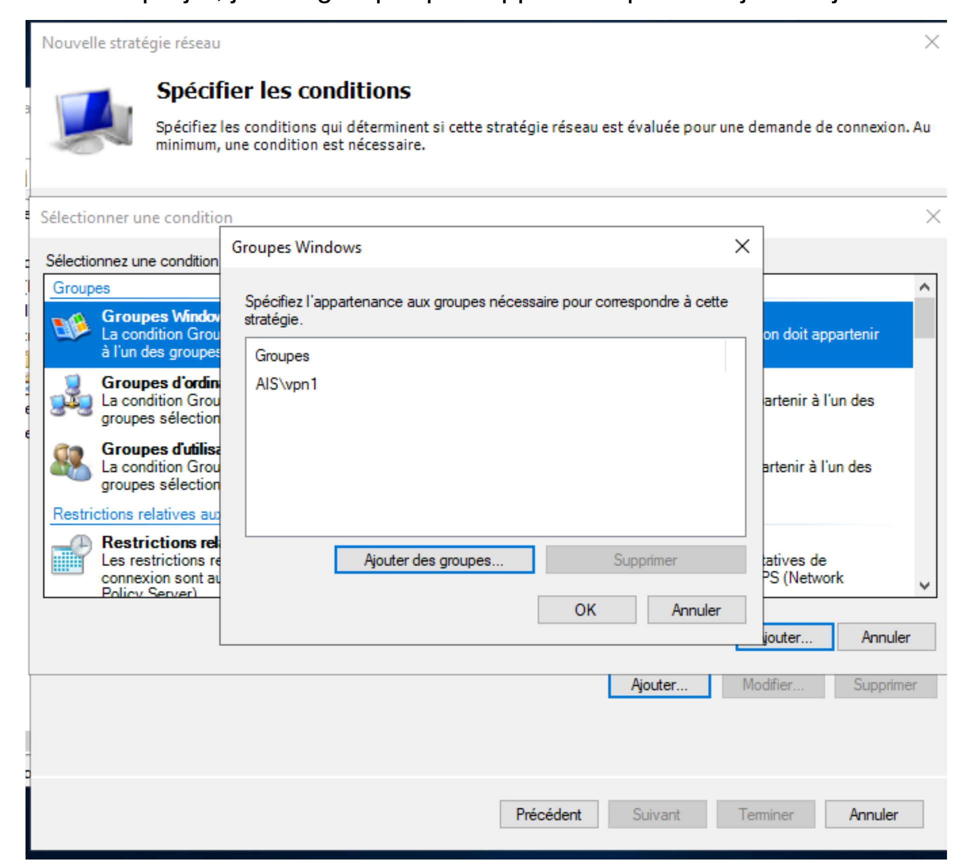
Il faut choisir un nom pour la stratégie et choisir la méthode de connexion :



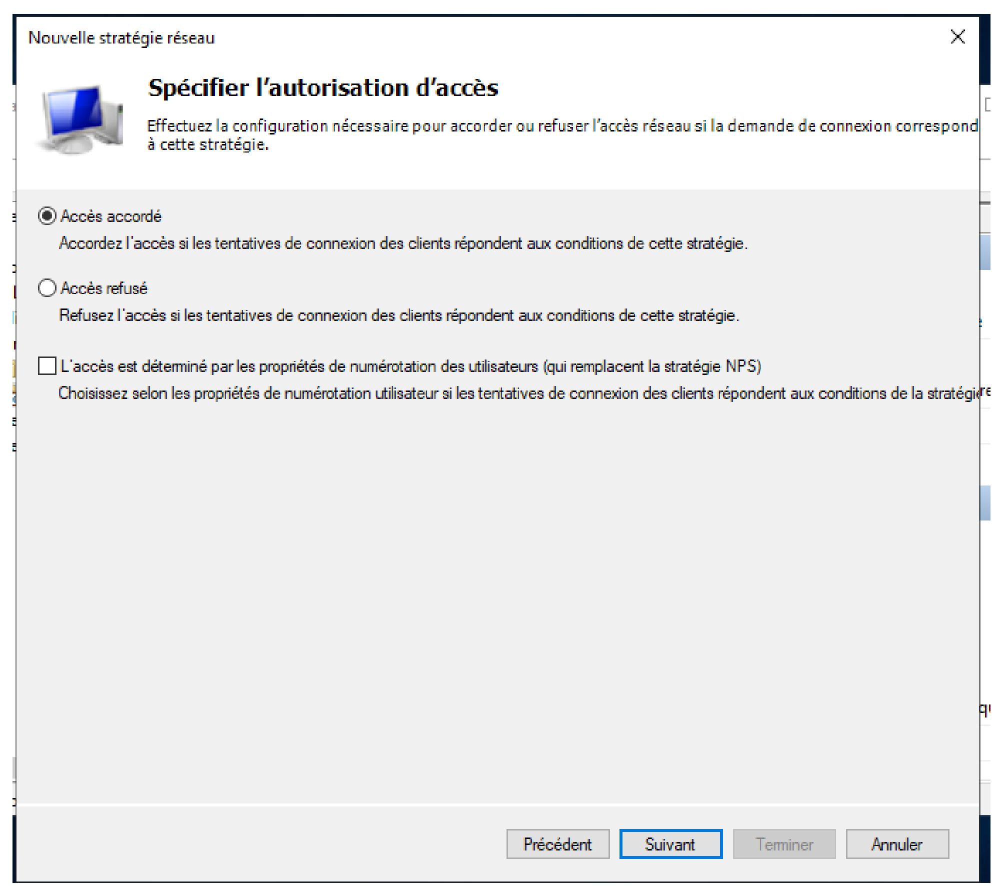
Ensuite, on doit ajouter notre groupe organisationnel qui utilise le VPN sur le NPS :



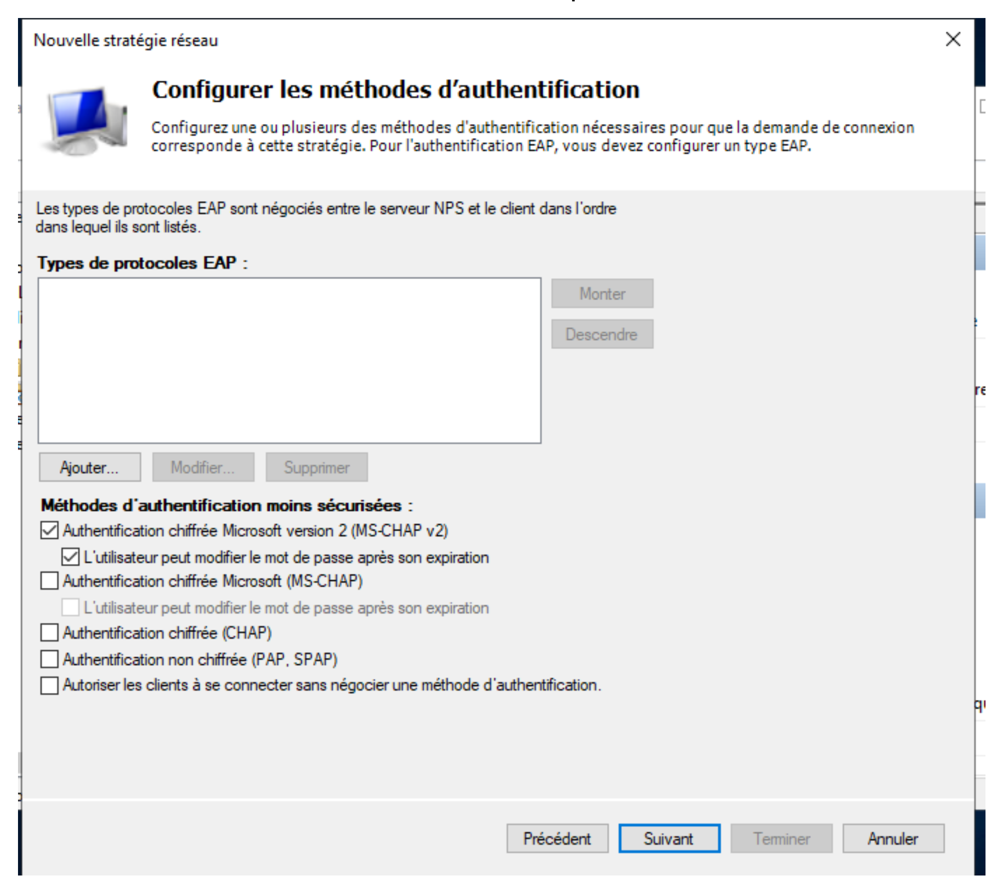
Dans ce projet, j'ai un groupe qui s'appelle « vpn1 » et je l'ai ajouté sur le NPS :



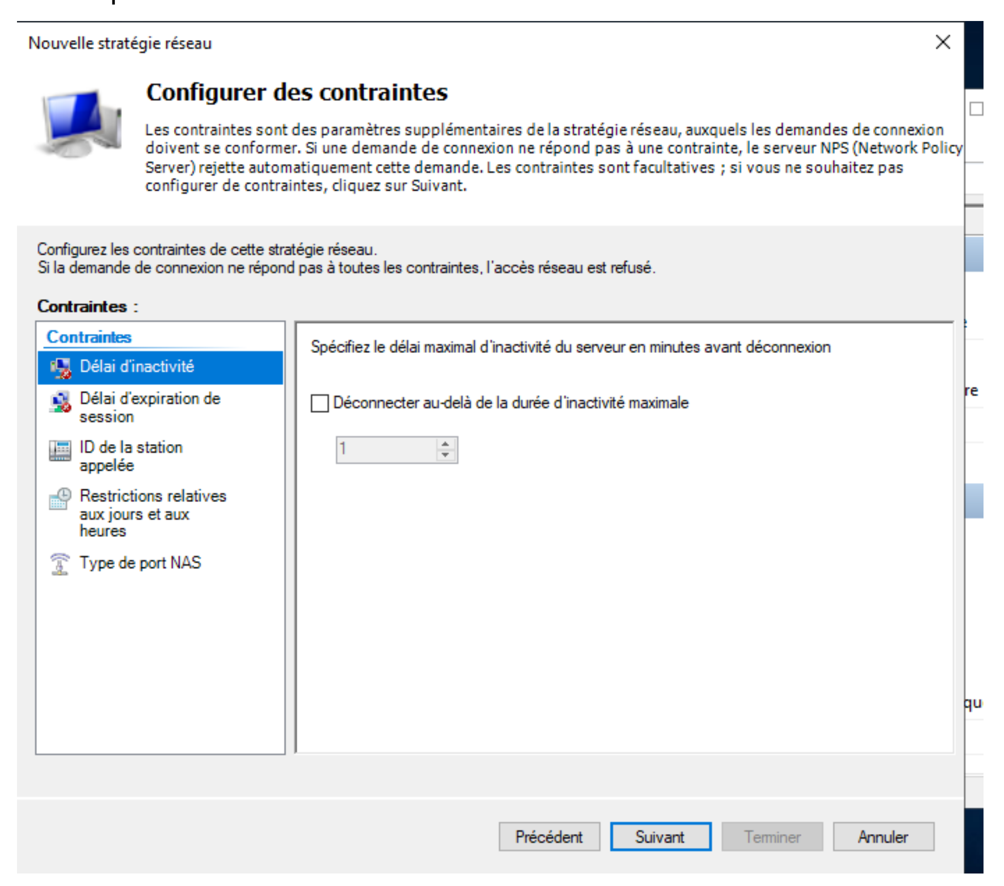
On accorde l'accès à ce groupe :



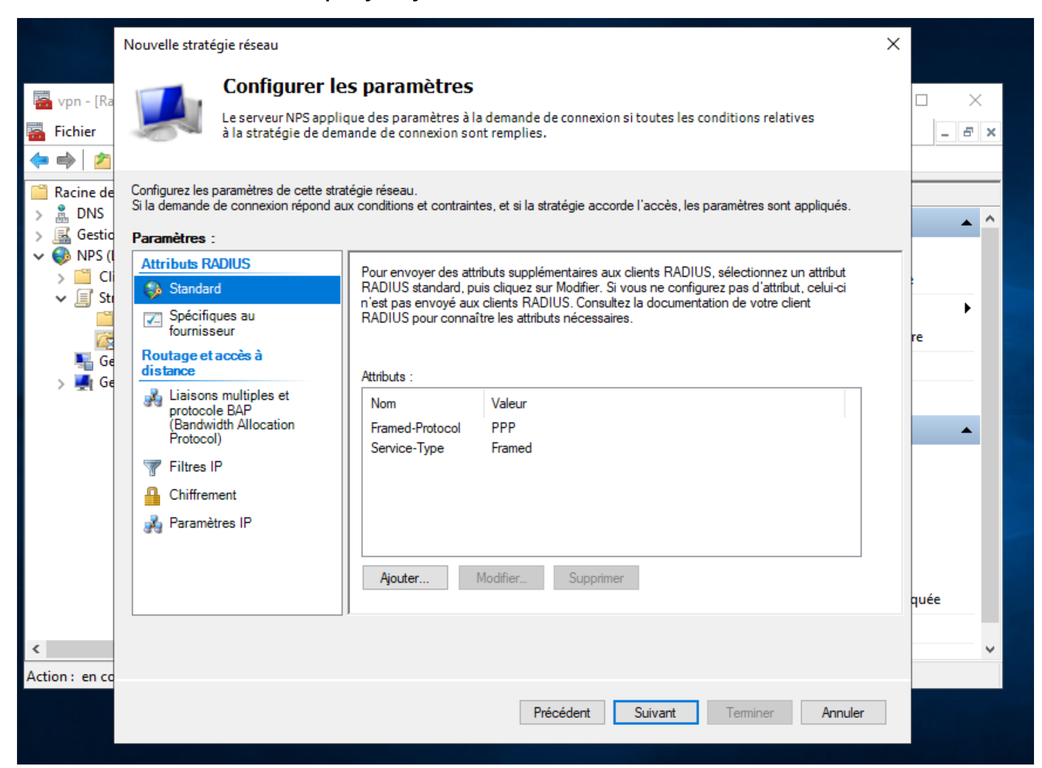
On sélectionne le mode de chiffrement de préférence MS-CHAP v2.



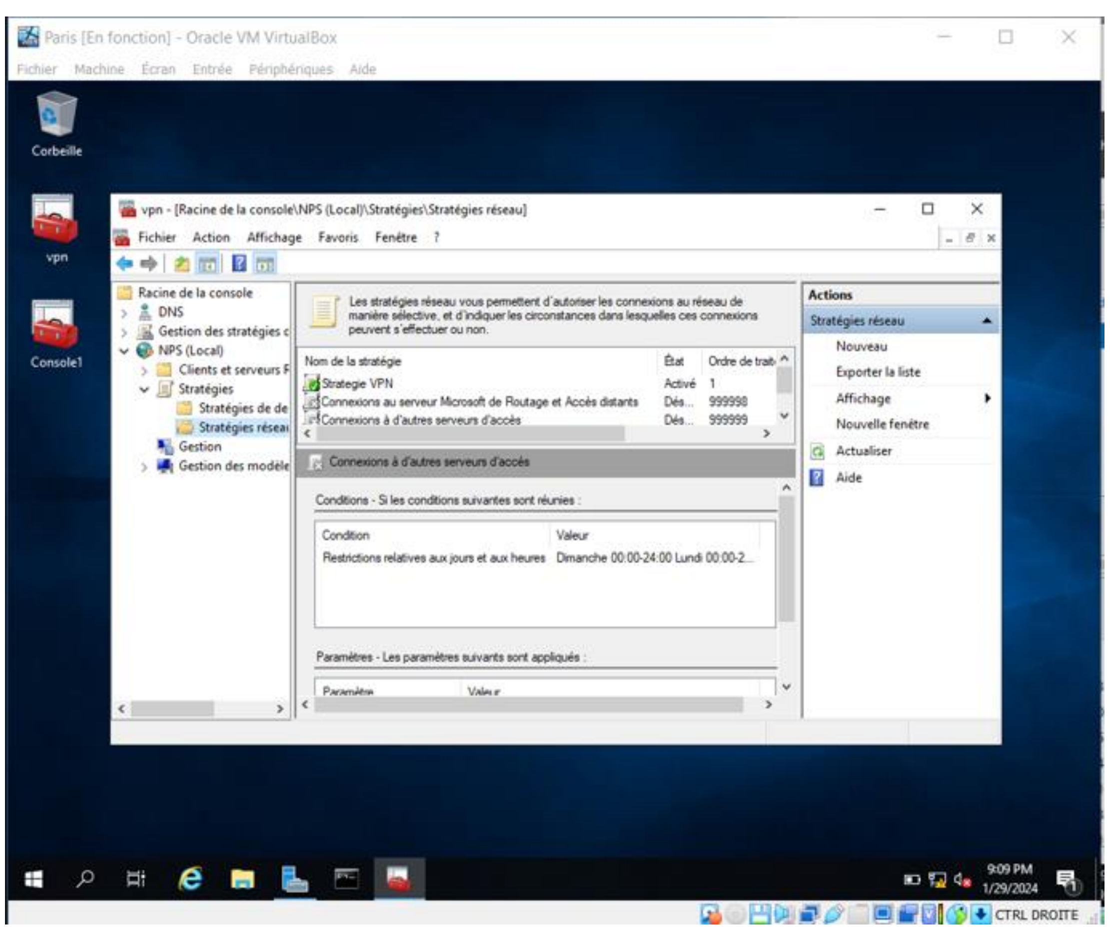
Ici, on peut déterminer des conditions des profils pour déterminer l'autorisation des utilisateurs et des dispositifs.



Dans le contexte de ce projet, j'utilise les attributs RADIUS :



Stratégie crée :



3.2 Configuration des clients RADIUS

Configurons maintenant les clients RADIUS avec les informations nécessaires, notamment l'adresse IP du client et la clé partagée.

On clique sur Clients et serveurs RADIUS et ensuite sur configurer les clients RADIUS :

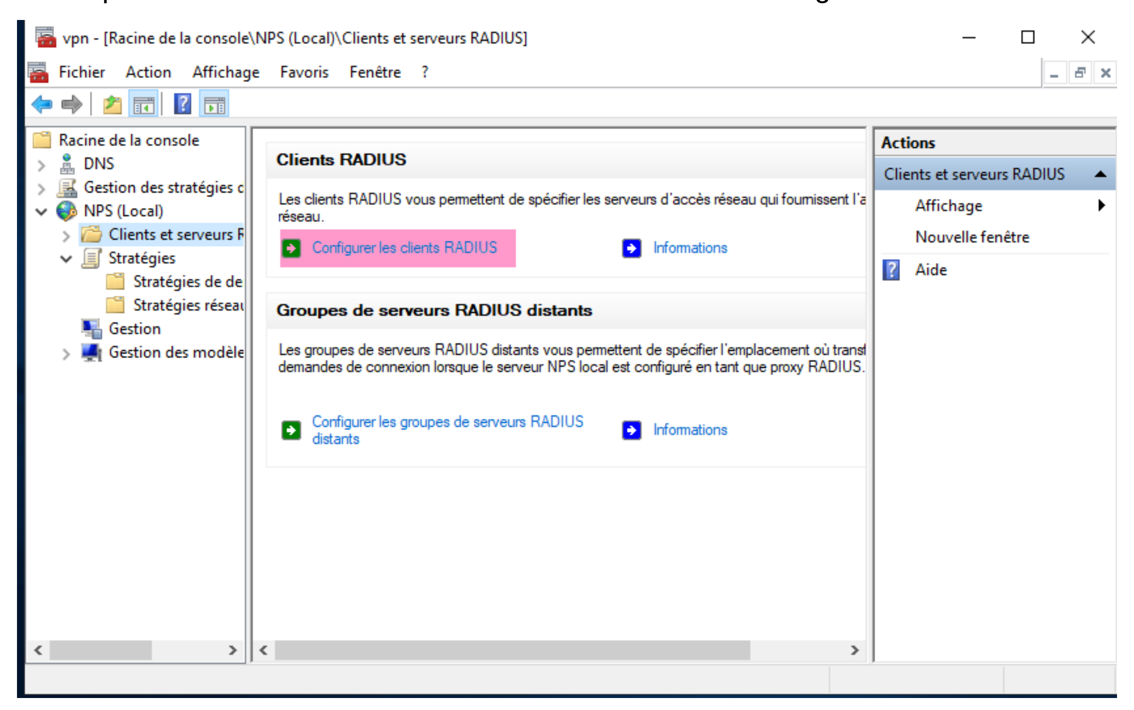
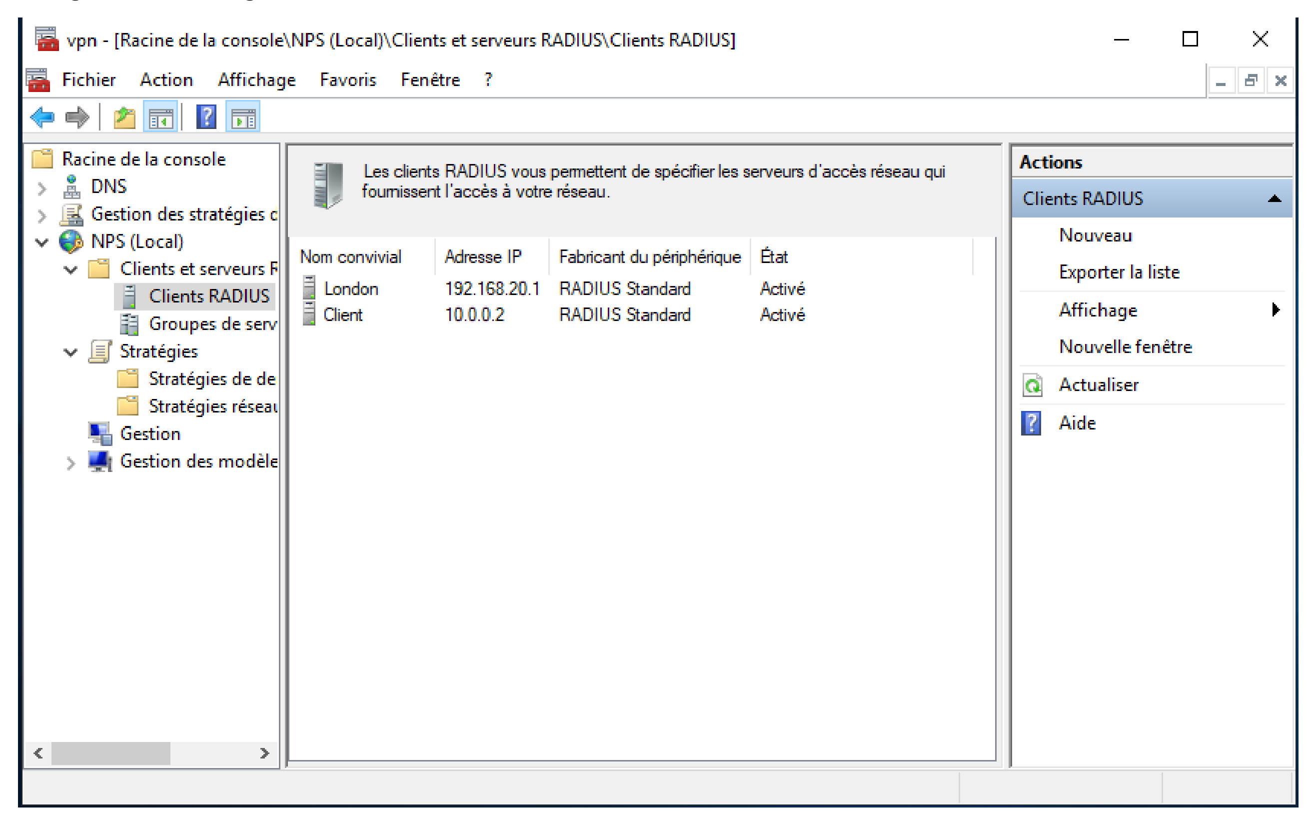
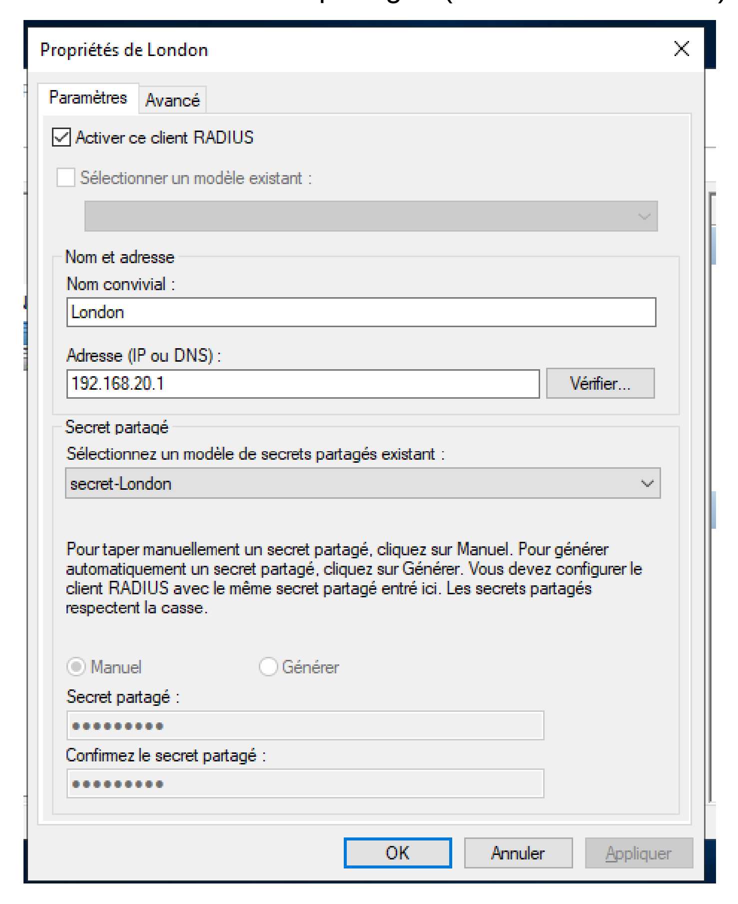


Image de la configuration faite :



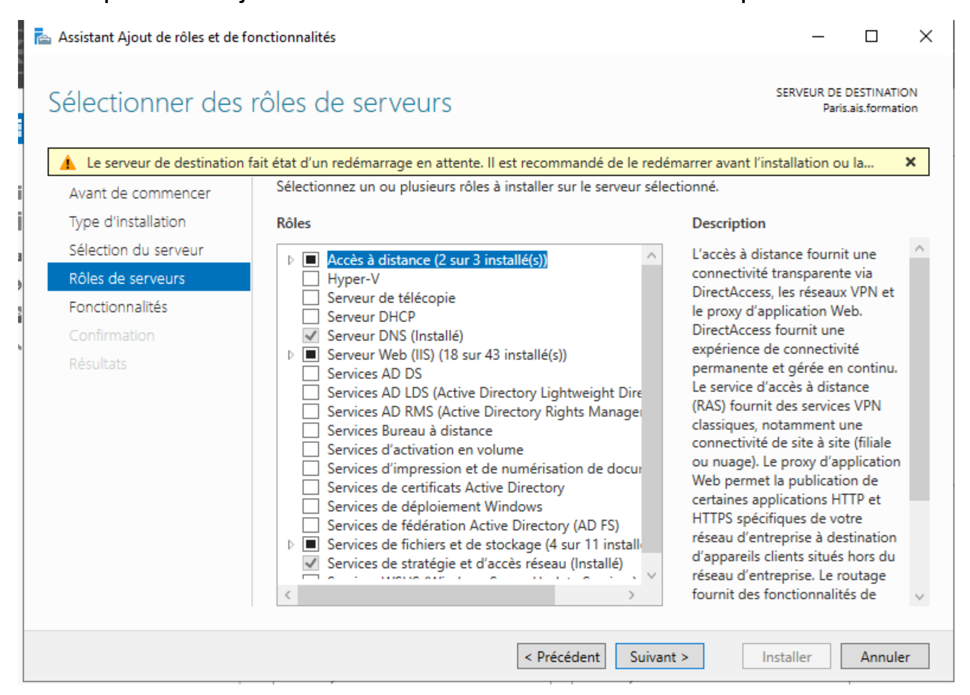
Modèle crée d'une clé partagée (selon le TP RADIUS) :



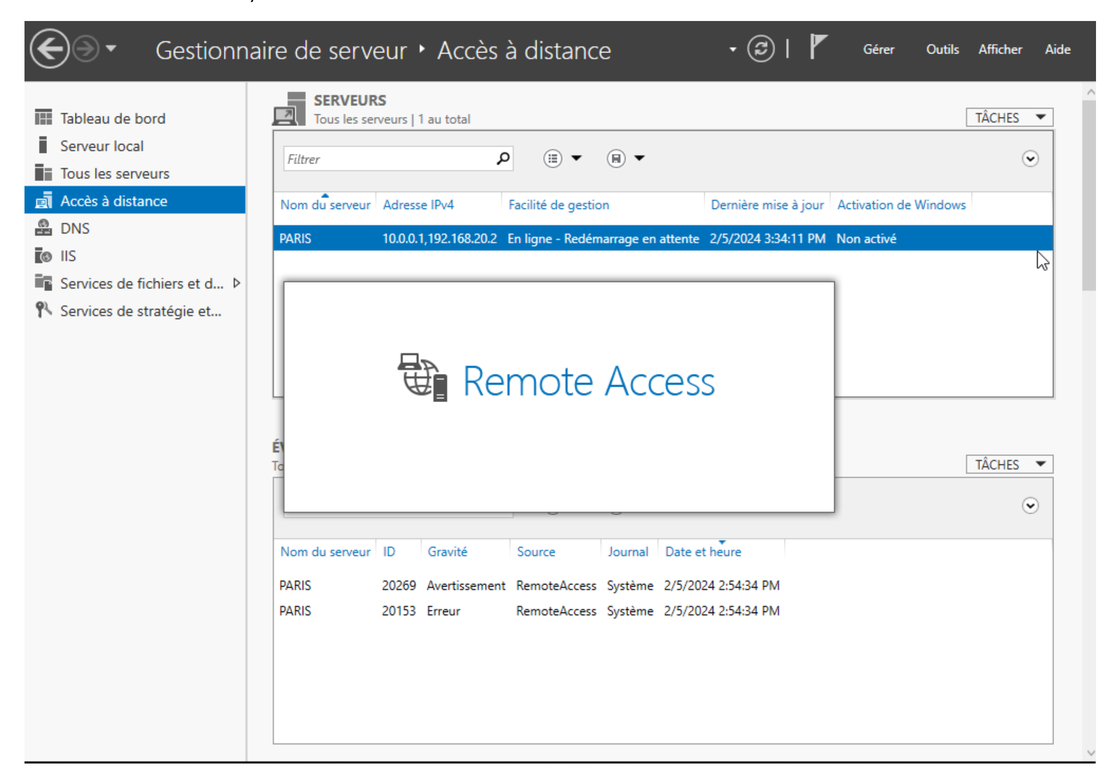
4. Installation de la fonctionnalité d'Accès à distance

La fonctionnalité "Accès à distance" sur un serveur Windows offre des moyens sécurisés et flexibles pour permettre aux utilisateurs de se connecter et d'interagir avec le serveur à partir de sites distants, contribuant ainsi à la mobilité et à la gestion à distance des systèmes informatiques.

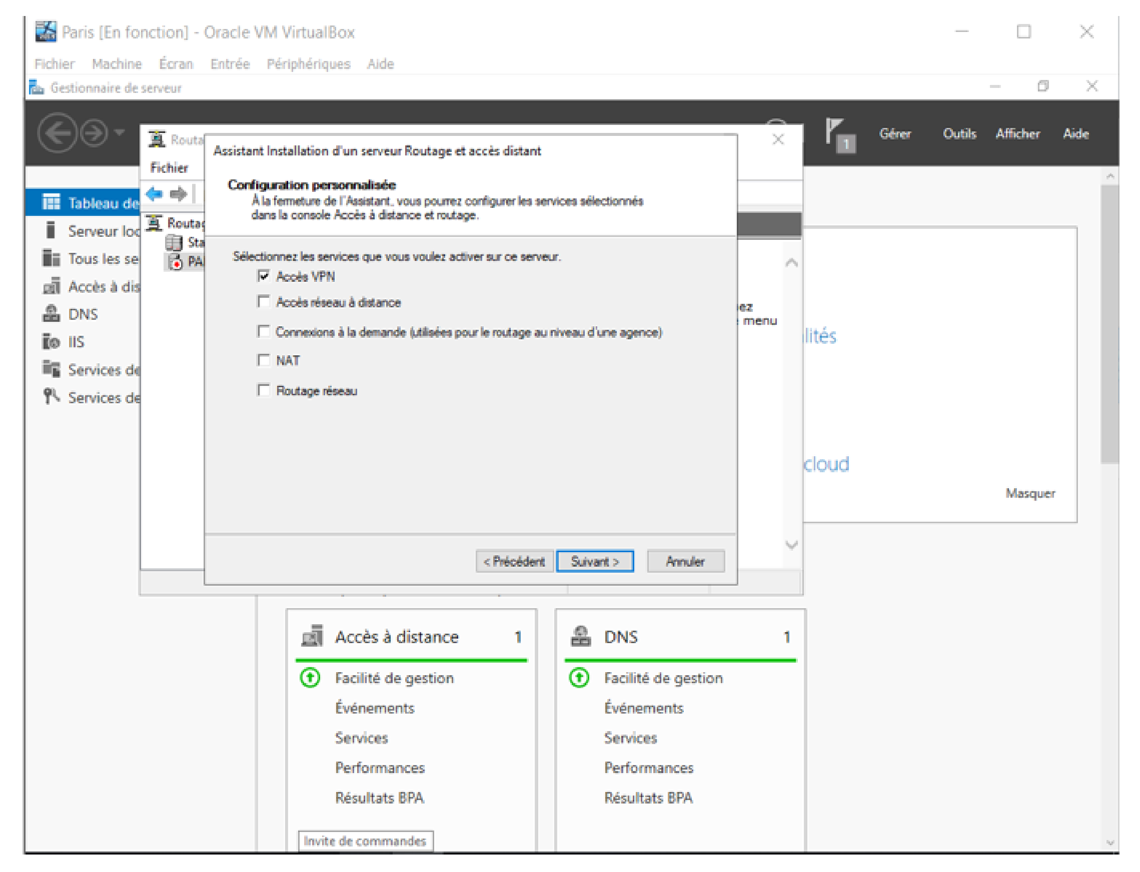
On clique sur « ajouter un rôle ou fonctionnalité » et on procède à l'installation des services RDS.



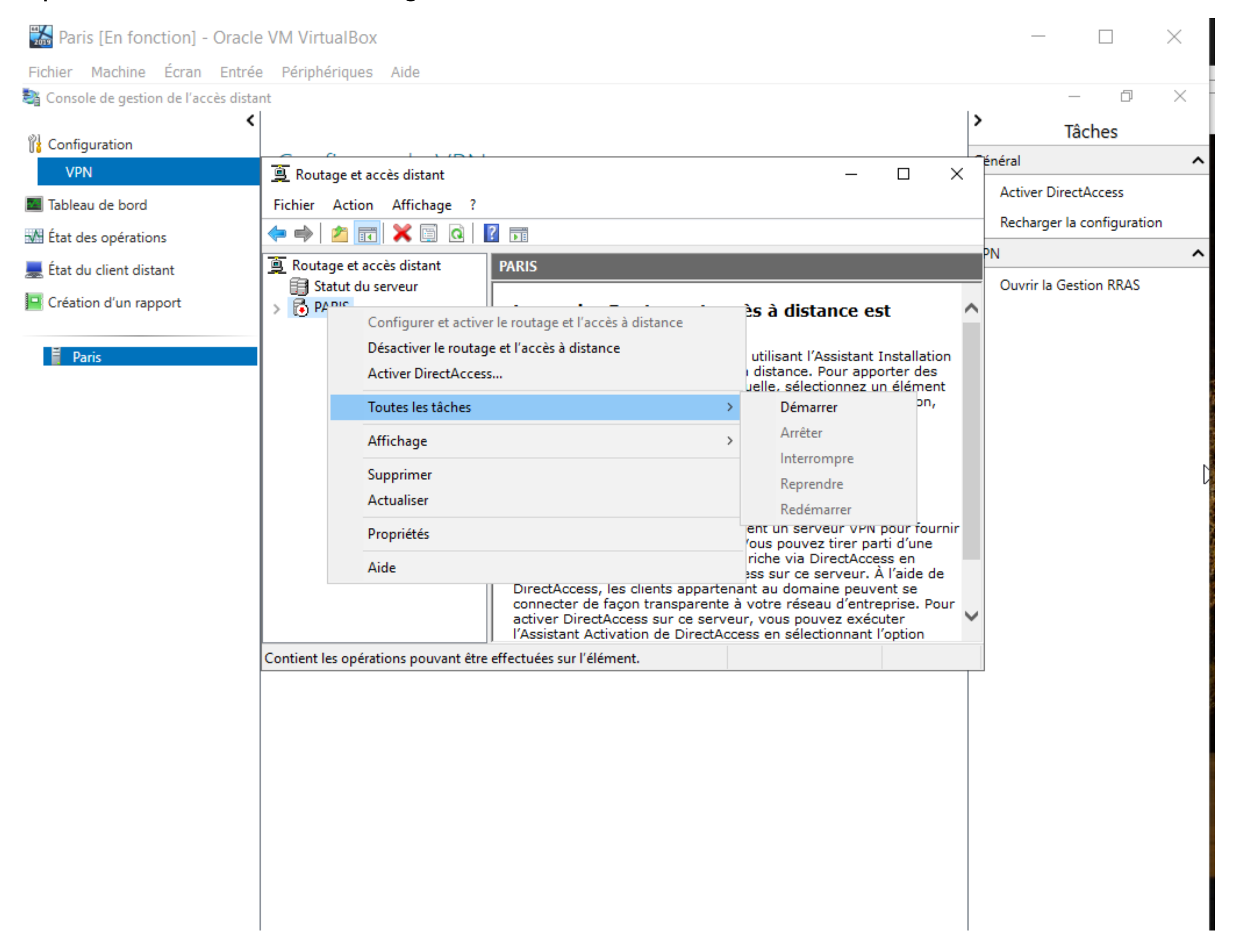
Une fois installée, on accède à l'outil :



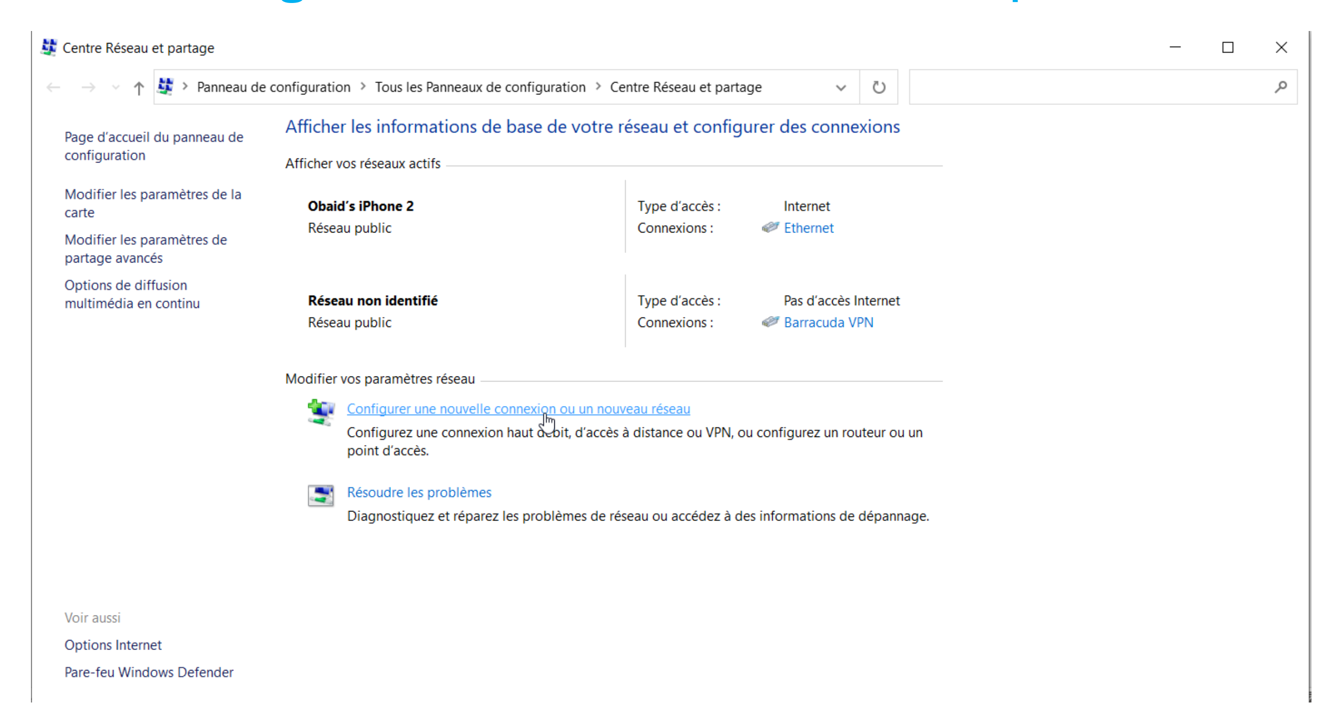
Ainsi, configurons maintenant le serveur :



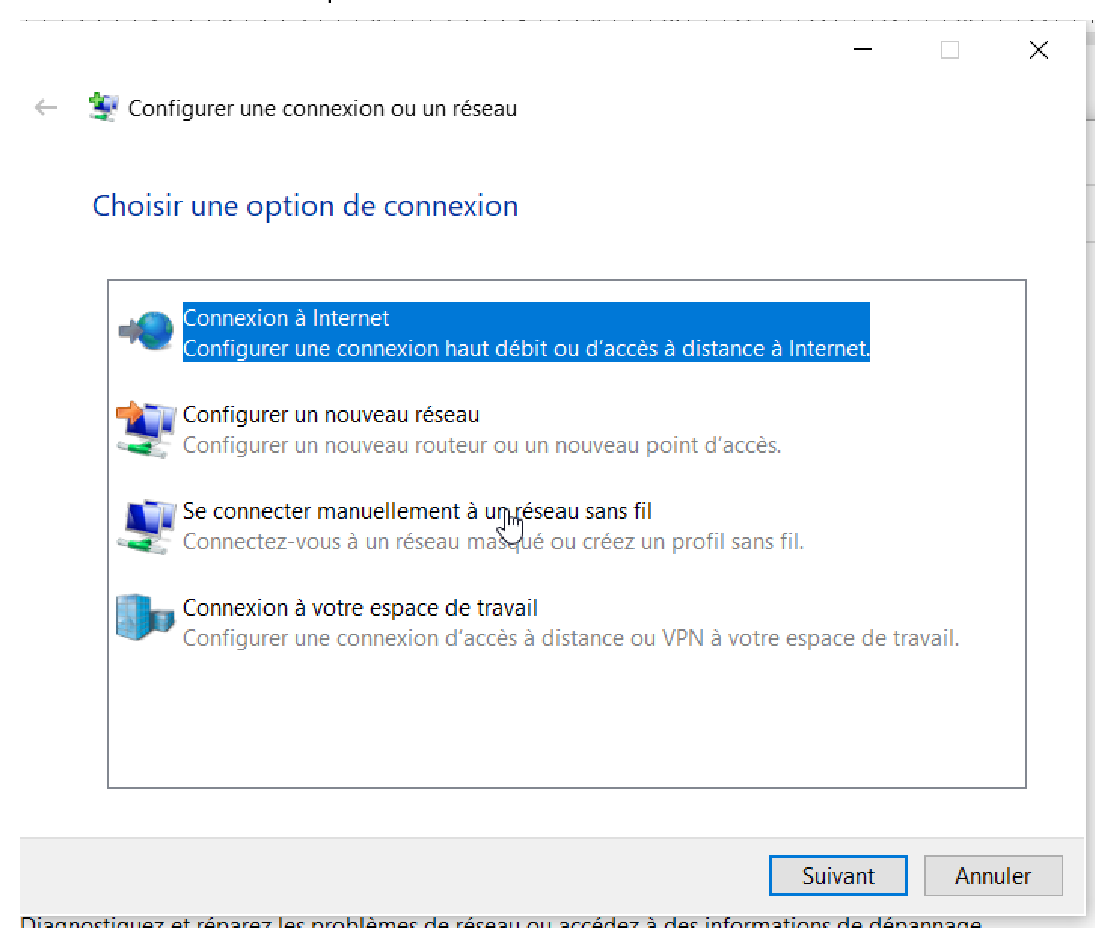
Après la finalisation des configurations, on démarre le service :



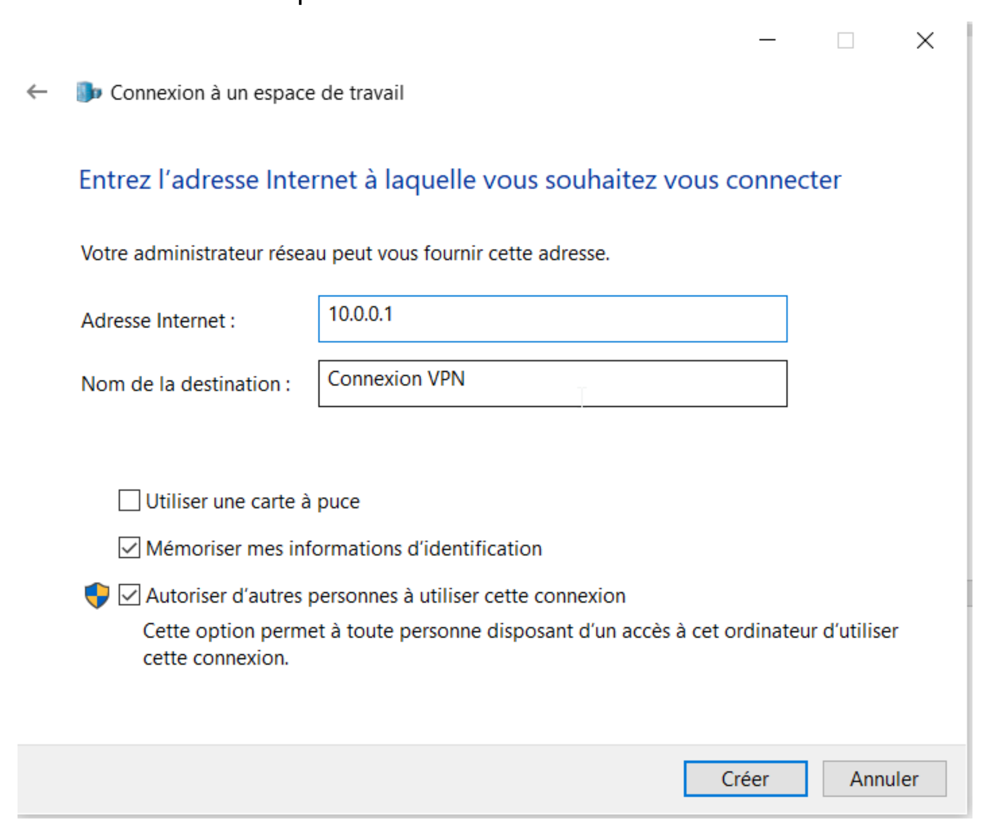
5. Configuration d'une connexion via le compte client



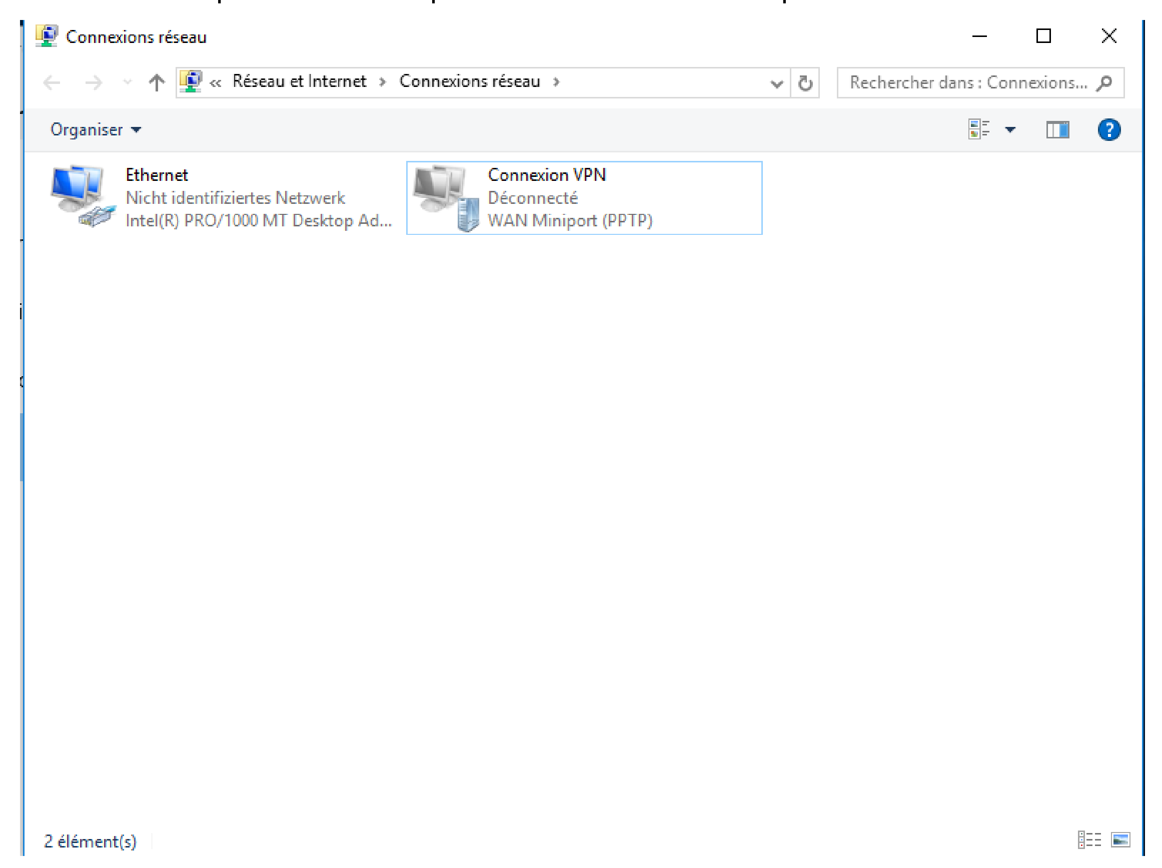
On se connecte sur l'espace de travail :



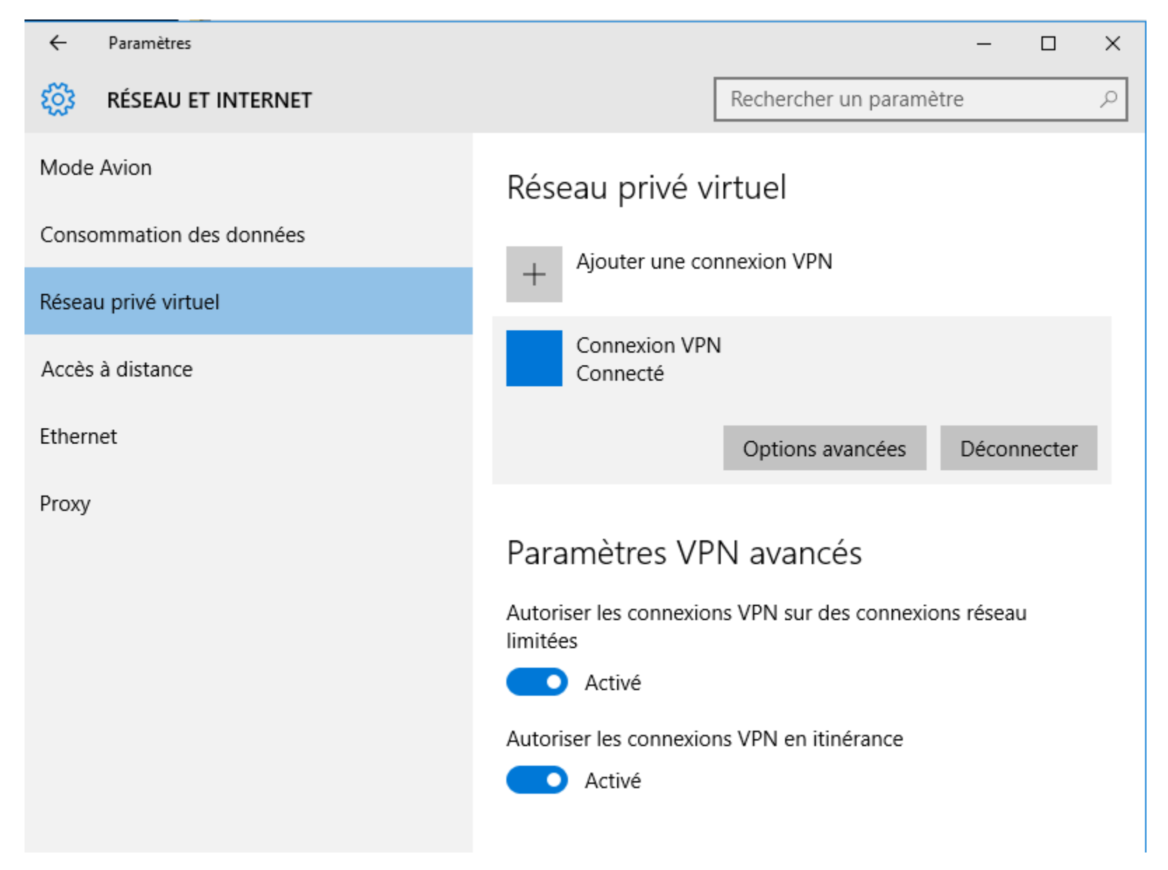
Connexion à notre espace de travail :



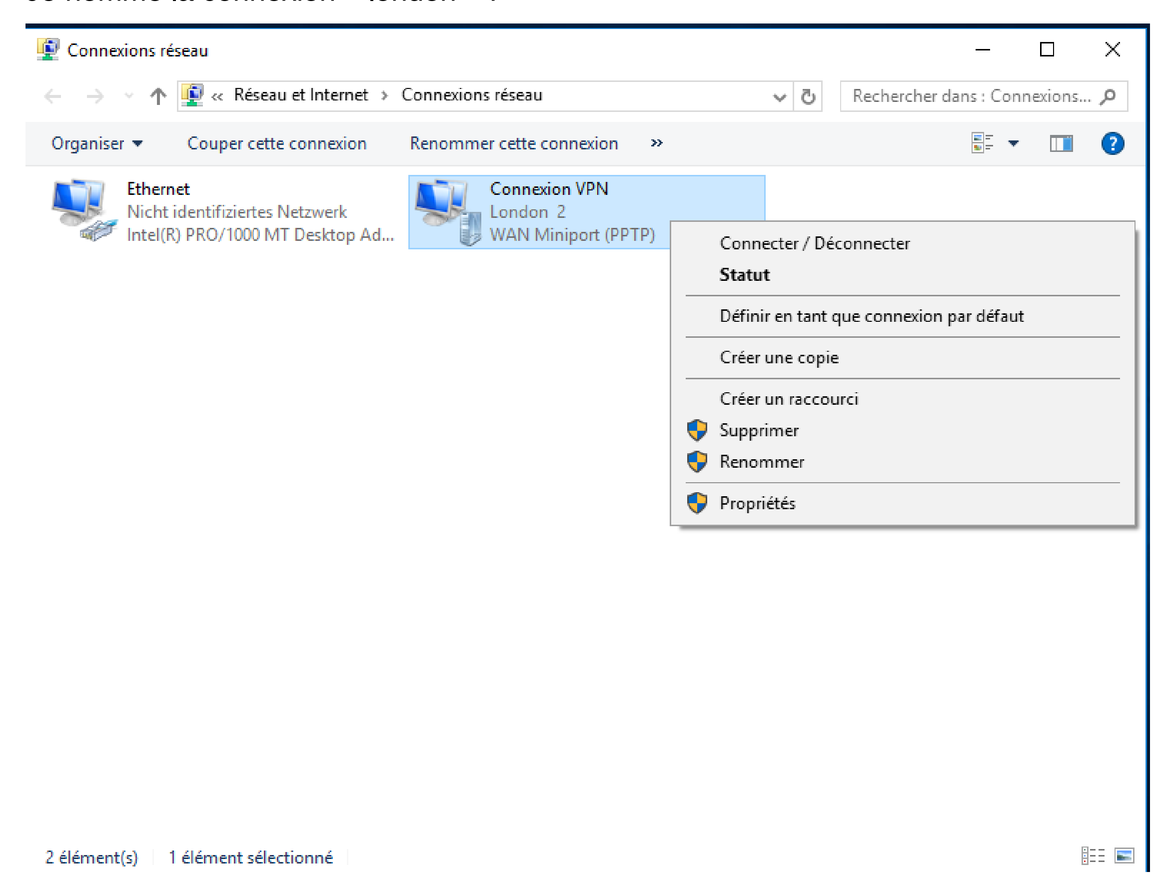
Il faut utiliser le protocole PPTP pour cette connexion mais pas IKeV2.



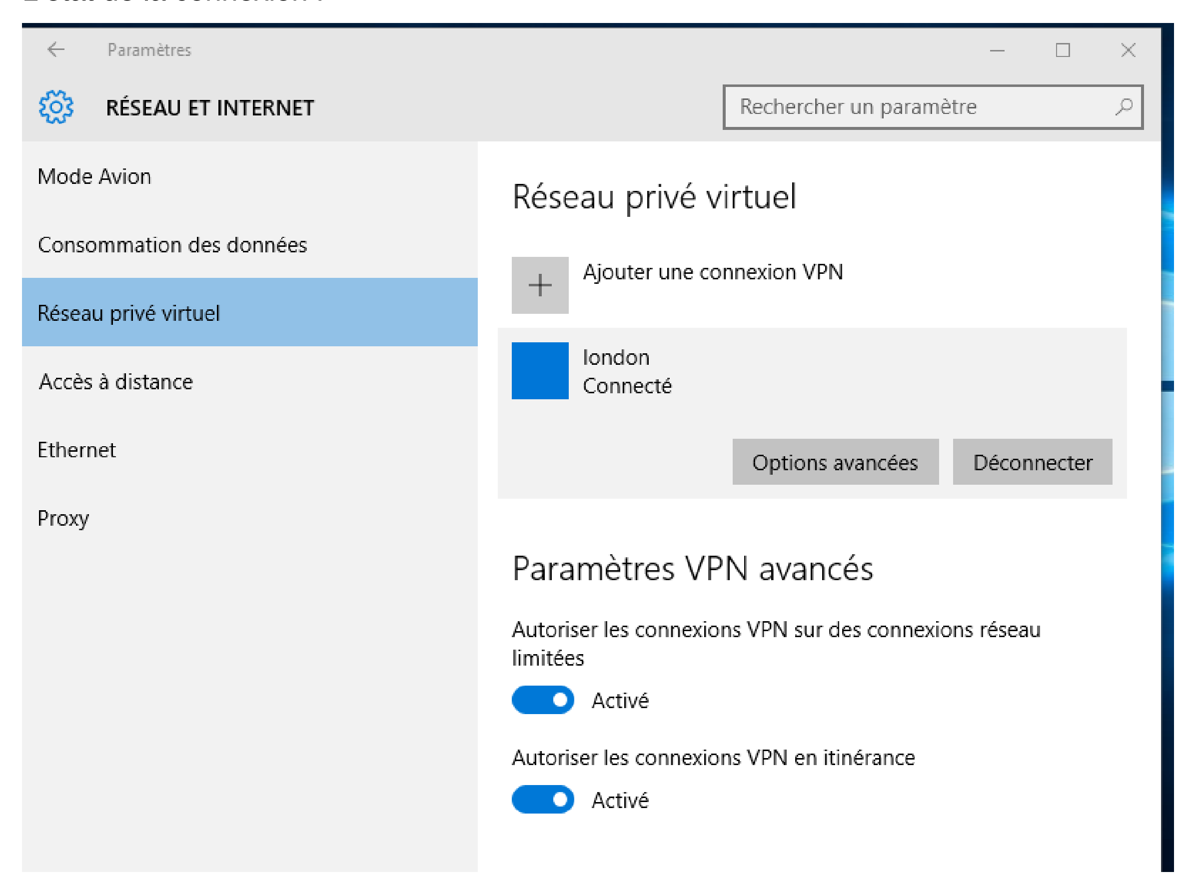
La connexion a été établi :



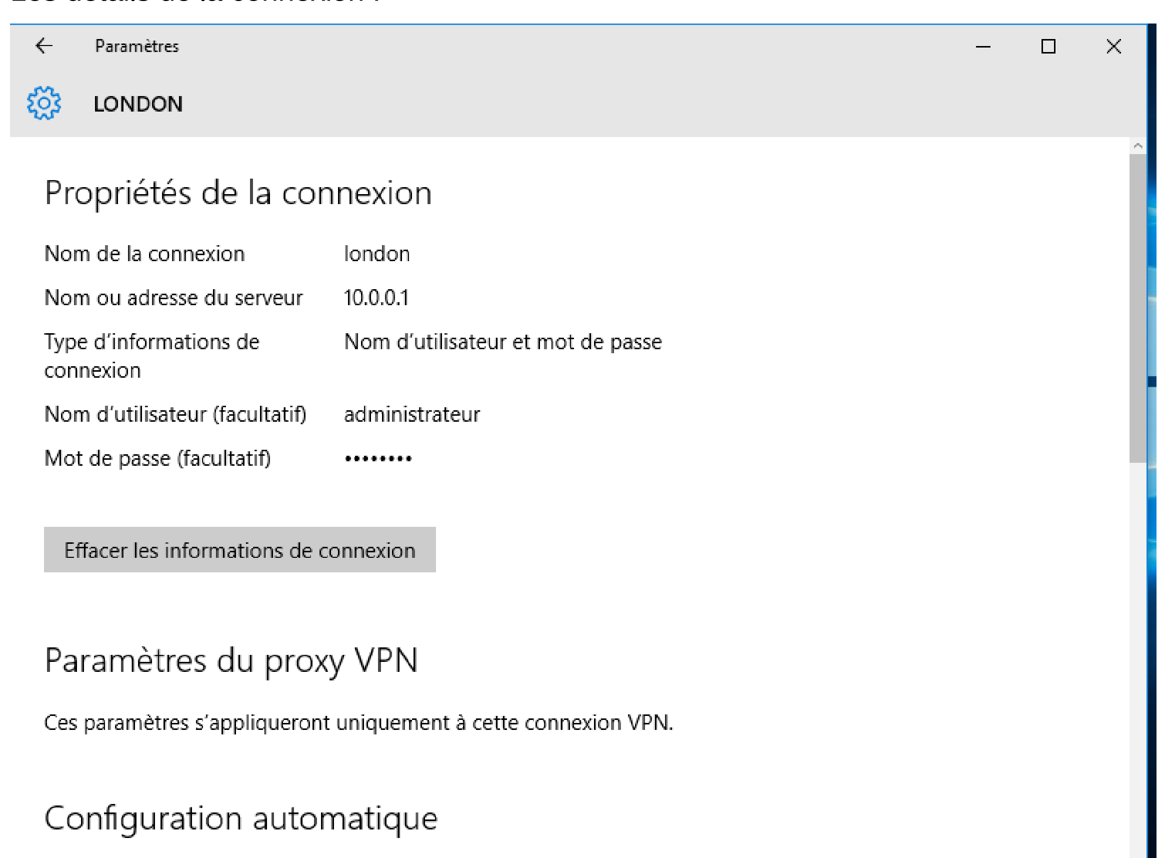
Je nomme la connexion « london » :



L'état de la connexion :



Les détails de la connexion :



Je peux accéder au serveur « London » depuis le compte client 10.0.0.2.

